AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

1. (Withdrawn) A method for verifying a digital signature used for verifying a digital signature of a message, wherein

a digital signature former side apparatus has:

a signature forming step in which a secret key owned by a digital signature former acts on the message or a hash value of the message to form a digital signature on the message, and

a registration step in which the message with digital signature including the formed digital signature and message is delivered and log data of the message with digital signature is registered in a log list, and

a digital signature verifier side apparatus has:

a verification target acceptance step for accepting the delivered message with a digital signature as a message with a verification target digital signature,

a history acquisition step for acquiring a log list of a digital signer to whom the message with a verification target digital signature has been delivered, and

a history existence verification step in which whether or not log data of the message with a verification target digital signature is registered in the log list is checked, and

if a check result is YES, additionally has:

an individual reliability setting step in which the reliability of the log data included in the log list is set,

a history reliability calculation step in which reliability of the log list is calculated based on the set individual reliability, and

a verification step in which a fact that the message with a verification target digital signature is delivered from the digital signature former side apparatus is authenticated with reliability.

2. (Withdrawn) An apparatus for verifying a digital signature comprising:

verification target acceptance means for accepting a message with a verification target digital signature,

history acquisition means for acquiring a log list of a digital signer to whom the message with a verification target digital signature has been delivered,

history existence verification means for checking whether or not log data of the message with a verification target digital signature is registered in the log list,

individual reliability setting means for setting reliability of the log data included in the log data if the log data of the message with a verification target digital signature is registered,

history reliability calculation means for calculating reliability of the log list based on the set individual reliability, and

verification means for authenticating with reliability a fact that the message with a verification target digital signature is delivered from the digital signature former side apparatus.

3. (Withdrawn) A method for arbitration used for solving a dispute on a digital signature of a message, wherein the method for arbitration comprises:

a request acceptance step in which a message with an arbitration target digital signature is accepted from an arbitration requestor apparatus,

a step in which a log list of the message with an arbitration target digital signature is acquired,

a step in which a fact that the message with a digital signature that has been requested for verification has been formed by a digital signature former side apparatus is verified by use of the acquired log list of the digital signer, and

an arbitration step in which an arbitration result is output based on reliability that is an output in the verification step.

4. (Withdrawn) An arbitrator apparatus for solving a dispute on a digital signature of a message comprising:

request acceptance means for accepting a message with an arbitration target digital signature,

history acquisition means for acquiring a log list of the message with an arbitration target digital signature,

history existence verification means for checking whether or not the log data of the message with an arbitration target digital signature is registered in the log list,

individual reliability setting means for setting the reliability of the log data included in the log data if the log data of the message with an arbitration target digital signature is registered,

history reliability calculation means for calculating reliability of the log list based on the set individual reliability, and

arbitration means for outputting an arbitration result based on the reliability.

5. (Previously Presented) A method for managing a log list, which is an issuing history of a digital signature issued on a message by a digital signature issue side apparatus, in a signature history storage service apparatus comprising:

accepting the log list from the digital signature issue side apparatus,

verifying validity of the digital signature of a digital signer signed on the log list or log list registration request data,

verifying consistency between the accepted log list and a registered log list of a registered digital signer,

adding and registering the accepted log list with the confirmed consistency to the registered log list of the digital signer, and

registering a user of the signature history storage service apparatus who is a digital signer of the digital signature issue side apparatus.

6. (Previously Presented) The method for managing a log list according to claim 5, further comprising:

confirming the consistency is confirmed, and

transmitting a fact that the accepted log list is added and registered to the registered log list of the digital signer, to a digital signer side apparatus.

7. (Previously Presented) The method for managing a log list according to claim 5 comprising:

a step in which the digital signature issue side apparatus requests registration of the accepted log list to the signature history storage service apparatus, and

a step in which log data other than the newest log data included in the accepted log list is deleted if the additional registration notice is received.

8. (Previously Presented) The method for managing a log list according to claim 7, wherein

the digital signature issue side apparatus performs:

a step comprising issuing electronic data of a deposition request document for indicating intention of a registration request, and

a step comprising transmitting the issued deposition request document electronic data, a public key certificate, and log list data, to the signature history storage service apparatus and

as the step for verifying the validity of the digital signature, the signature history storage service apparatus performs:

a step comprising verifying the validity of the received public key certificate, and

a step comprising checking whether or not the deposition request document is verified correctly by use of a public key of a user included in the public key certificate.

9. (Previously Presented) The method for managing a log list according to claim 7, wherein the digital signature issue side apparatus requests registration of the log list every time when a digital signature is issued.

10. (Withdrawn) A method for verifying a digital signature in which a log list storage side apparatus verifies a digital signature that a digital signature former side apparatus has formed on a message, wherein the digital signature apparatus has:

a signature forming step in which a secret key owned by the digital signature former acts on the message or a hash value of the message to form a digital signature on the message,

a registration step in which log data of the message with a digital signature is registered in a log list, and

a step in which registration of the log list is requested to the log list storage side apparatus,

the log list storage side apparatus has:

a step in which the log list registration request is accepted from the digital signature former side apparatus,

a step in which effectiveness of the digital signature formed by the digital signer signed on the log list or the log list registration request included in the log list registration request is verified,

a step in which consistency between the accepted log list and a log list of the digital signer that has already been registered is verified,

a step in which a verification request of the message with a digital signature is accepted from the external, and

a step in which a fact that the message with a digital signature that has been requested for the verification has been formed by the digital signature former side apparatus is authenticated by use of the registered log list of the digital signer.

11. (Withdrawn) The method for verification according to claim 10 wherein

the digital signature former side apparatus has:

a step in which the formed digital signature and the message with a digital signature including the message are transmitted to the digital signature receiver side apparatus additionally,

the digital signature receiver side apparatus has:

a step in which the message with a digital signature is received, and

a step in which verification vicarious execution of the message with a digital signature is requested to the log list storage side apparatus, and

the log list storage side apparatus has:

a step in which the verification request of the message with a digital signature that the digital signature receiver side apparatus has received from the digital signature former side apparatus is accepted from the digital signature receiver side apparatus.

12. (Withdrawn) The method for verification according to claim 10, wherein the log list storage side apparatus registers the digital signature on the log list after correctness of the digital signature is confirmed in the verification step.

13. (Withdrawn) The method for verification according to claim 10, wherein the log list storage side apparatus has:

a step in which a verification vicarious execution request is received from a verification vicarious execution requestor apparatus, and

a step in which a verification result is transmitted to the verification vicarious execution requestor apparatus.

14. (Withdrawn) The method for verification according to claim 10, wherein the log list storage side apparatus accepts the log list registration request from the plural digital signature former side apparatuses.

15. (Withdrawn) The method for verification according to claim 11, wherein each step carried out in the digital signature receiver side apparatus is carried out in an arbitration

requestor apparatus used by an arbitration requestor who requests arbitration of correctness of a signature formed by the signer.

16. (Withdrawn) A log list storage side apparatus for verifying a digital signature formed in a digital signature former apparatus comprising:

a memory unit for registering a log list,

reception means for accepting log list registration request from the digital signature former side apparatus,

means for verifying effectiveness of a digital signature formed by the digital signer signed on the log list or the log list registration request included in the log list registration request,

means for verifying consistency between the accepted log list and a log list of the digital signer registered in the memory unit,

verification means for authenticating a fact that the message with a digital signature that has been requested for the verification vicarious execution has been formed by the digital signature former side apparatus by use of the registered log list of the digital signer registered in the memory unit, and

transmission means for transmitting a verification result to the external.

17. (Withdrawn) The method for arbitration according to claim 3, wherein the method comprises:

a step in which a management apparatus that manages a log list of a message with an arbitration target digital signature is requested for the log list, and

a step in which the log list of the message with an arbitration target digital signature is acquired from the management apparatus.

18. (Withdrawn) The log list storage side apparatus according to claim 16, wherein the memory unit registers the digital signature having consistency that has been confirmed by the verification means to the log list additionally therein.

19. (Withdrawn) The log list storage side apparatus according to claim 16, wherein:

the reception means accept a verification vicarious execution request of the received message with a digital signature from the digital signature receiver side apparatus that has received the digital signature formed and transmitted by the digital signature former side apparatus, and

the transmission means transmit a verification result to the digital signature receiver side apparatus.

20. (Currently Amended) ~~A method~~ The method of claim 5 for managing a log list, which is an issuing history of a digital signature issued on a message by a digital signature issue side apparatus, in a signature history storage service apparatus, further comprising:

~~accepting the log list from the digital signature issue side apparatus,~~

~~verifying validity of the digital signature of the digital signer signed on the log list or log list registration request data,~~

~~verifying consistency between the accepted log list and a registered log list of the registered digital signer, and~~

~~adding and registering the accepted log list with the confirmed consistency to the registered log list of the digital signer,~~

sending an additional registration notice to the digital signature issue side apparatus after registering the accepted log list to the registered log list, and

deleting in the digital signature issue side apparatus log data other than the newest log data ~~the log data thereafter necessary for verification of validity of the digital signature~~ of the digital signer included in the accepted log list when the digital signature issue side apparatus receives the additional registration notice sent from the signature history storage service apparatus.

21. (Previously Presented) The method for managing a log list according to claim 20, wherein

the digital signature issue side apparatus performs:

a step comprising issuing electronic data of a deposition request document for indicating intention of a registration request, and

a step comprising transmitting the issued deposition request document electronic data, a public key certificate, and log list data, to the signature history storage service apparatus, and

the step for verifying the validity of the digital signature, the signature history storage service apparatus performs:

a step comprising verifying the validity of the received public key certificate, and

a step comprising checking whether or not the deposition request document is verified correctly by use of a public key of a user included in the public key certificate.

22. (Previously Presented) The method for managing a log list according to claim 20, wherein the digital signature issue side apparatus requests registration of the accepted log list every time when a digital signature is issued.

23. (Previously Presented) The method for managing a log list according to claim 20, wherein said verifying consistency is performed by calculating a hash value h (Rn') of the signature issuing record Rn', and confirming that the hash value h (Rn') in the signature issuing record Rn'+1 is identical with the calculated h (Rn').